



04 CO  
11-06-01

~~0500~~

Docket No. 500.40788X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): NINOMIYA, et al  
Serial No.: 09/981,760  
Filed: October 19, 2001  
Title: CRYPTOGRAPHIC KEY MANAGEMENT METHOD

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of  
Patents and Trademarks  
Washington, D.C. 20231

November 1, 2001

Sir:

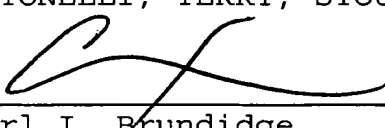
Under the provisions of 35 USC 119 and 37 CFR 1.55, the  
applicant(s) hereby claim(s) the right of priority based on:

Japanese Patent Application No. 2001-071581  
Filed: March 14, 2001

A certified copy of said Japanese Patent Application is  
attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

  
\_\_\_\_\_  
Carl I. Brundidge  
Registration No. 29,621

CIB/gfa  
Attachment



日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2001年 3月14日

出願番号

Application Number:

特願2001-071581

出願人

Applicant(s):

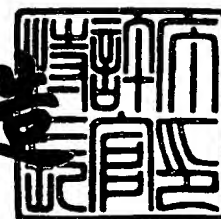
株式会社日立製作所

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 9月28日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3089312

【書類名】 特許願

【整理番号】 H0000589

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 5 0 3 0 番地 株式会社日立製作所 ソフトウェア事業部内

【氏名】 二宮 敏彦

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 5 0 3 0 番地 株式会社日立製作所 ソフトウェア事業部内

【氏名】 松永 和男

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100096954

【弁理士】

【氏名又は名称】 矢島 保夫

【手数料の表示】

【予納台帳番号】 022781

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 公開鍵管理方法

【特許請求の範囲】

【請求項 1】

クライアントからネットワーク経由でアプリケーションサーバに接続し各種の取引を行う際に使用する前記クライアントの公開鍵を管理する公開鍵管理方法であって、

前記クライアントは、該クライアントで作成した前記アプリケーションサーバごとの取引用公開鍵ペアを暗号化するための管理用の暗号鍵を保持し、

前記ネットワークには、前記管理用の暗号鍵により暗号化された前記クライアントの取引用公開鍵ペアを格納するための鍵管理サーバを設置することを特徴とする公開鍵管理方法。

【請求項 2】

クライアントからネットワーク経由でアプリケーションサーバに接続し各種の取引を行う際に使用する前記クライアントの公開鍵を管理する公開鍵管理方法であって、

前記クライアントで、前記アプリケーションサーバごとの取引用公開鍵ペアを暗号化するための管理用の暗号鍵を作成し、保持するステップと、

前記クライアントで、前記アプリケーションサーバごとに取引用公開鍵ペアを生成するステップと、

前記クライアントで、前記生成した取引用公開鍵ペアを前記管理用暗号鍵で暗号化するステップと、

前記暗号化された取引用公開鍵ペアを、前記ネットワークに接続された鍵管理サーバに送信するステップと、

前記鍵管理サーバで受信した前記暗号化された取引用公開鍵ペアを所定の記憶手段に格納するステップと、

前記クライアントから前記アプリケーションサーバに接続して取引きするため、前記鍵管理サーバから前記暗号化された取引用公開鍵ペアを取得するステップと、

取得した取引用公開鍵ペアを、前記保持してある管理用暗号鍵で復号するステップと、

復号した取引用公開鍵ペアを用いて前記アプリケーションサーバとの取引を実行するステップと

を備えたことを特徴とする公開鍵管理方法。

【請求項3】

請求項1または2に記載の公開鍵管理方法において、

前記鍵管理サーバで、前記取引用公開鍵ペアの有効期限を管理し、該有効期限が満了したとき、または、該有効期限満了前の所定期間に至ったときに、前記クライアントに対して取引用公開鍵ペアの更新を行うべきことを通知するステップを、さらに備えたことを特徴とする公開鍵管理方法。

【請求項4】

請求項1または2に記載の公開鍵管理方法において、

前記鍵管理サーバで、前記取引用公開鍵ペアの使用回数、最終使用の日時、または使用履歴を管理し、これらの情報に基づいて不正な使用を検出するステップを、さらに備えたことを特徴とする公開鍵管理方法。

【請求項5】

請求項4に記載の公開鍵管理方法において、

不正な使用を検出したとき、前記取引用公開鍵ペアの使用を制限または禁止するステップを、さらに備えたことを特徴とする公開鍵管理方法。

【請求項6】

請求項1または2に記載の公開鍵管理方法において、

前記鍵管理サーバに格納する前記取引用公開鍵ペアのうち、公開鍵は平文で格納することを特徴とする公開鍵管理方法。

【請求項7】

請求項1、2、または6に記載の公開鍵管理方法において、

前記鍵管理サーバに前記クライアントの鍵管理用公開鍵をさらに保管し、前記取引用公開鍵ペアの使用時に、前記鍵管理用公開鍵を用いて個人認証を実施することを特徴とする公開鍵管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークを利用して電子商取引などを行う際に使用する鍵管理技術に関する。

【0002】

【従来の技術】

ネットワークを利用して電子商取引などを行う場合、相手を特定するための認証処理が必要である。認証処理には鍵（証明書）を利用するが、通常は、サービスを提供するアプリケーションサーバ毎に、個人が例えば取引用公開鍵ペア（公開鍵暗号技術により生成される公開鍵と秘密鍵のペア）を生成し、自分自身で管理して使い分けていた。したがって、例えばクレジットカード決済や銀行決済においては、取引引きするクレジットカード会社や銀行毎に、個人は別々の取引用公開鍵ペアを管理する必要があった。

【0003】

また、SET（Visa InternationalとMasterCard Internationalの策定したSecure Transaction Protocol）の推進団体であるSETCoに提案されている“Server-Based Wallet Security Proposal”に示されているようにWallet（消費者が使用する電子決済ソフトウェア）機能をサーバ側で実行し、個人クライアントからはWebブラウザでサーバ経由で電子商店などのアプリケーションサーバにアクセスする方法など、個人の鍵管理を代行するサーバを設置する方式があるが、これは代行するサーバでアプリケーションを実行してアプリケーションサーバと個人の接続を中継する方式である。

【0004】

特開2000-49766には、各個人がアプリケーションサーバ毎に鍵管理を行う負担を軽減するため、鍵管理サーバを設け、該鍵管理が鍵生成とアプリケーション用公開鍵証明書の取得を自動的に行う技術が開示されている。

【0005】

【発明が解決しようとする課題】

上述したように、各個人は、電子商取引などのサービスを提供するアプリケーションサーバ毎に鍵管理を行わなければならない管理の負担が少なくなかった。

【0006】

また、各個人で複数の取引用公開鍵ペアを保持する場合、それらの鍵を記憶しておく記憶手段に大きな容量が必要であるため、携帯端末からの取引が不可能である場合があった。

【0007】

上述の鍵管理をサーバで代行する技術によれば、アプリケーションサーバ毎の個人側のアプリケーション実行をサーバで代行するので、代行するサーバの負荷が大きい。また代行するサーバが個人の公開鍵ペアを管理するためセキュリティ上の問題があり、さらに高度のセキュリティを実現するためには代行するサーバの負担が非常に大きいという問題がある。

【0008】

さらに、特開2000-49766の技術では、取引用公開鍵ペアを作成・管理するのは鍵管理サーバであるため、セキュリティ上の問題がある。

【0009】

本発明は、サービスを提供するアプリケーションサーバ毎に鍵管理が必要な場合でも、各個人の鍵管理の負担を軽減し、かつ携帯端末からの取引も容易で、セキュリティも確保することができるような鍵管理方法を提供することを目的とする。

【0010】

【課題を解決するための手段】

上記目的を達成するため、本発明は、クライアントからネットワーク経由でアプリケーションサーバに接続し各種の取引を行う際に使用する前記クライアントの公開鍵を管理する公開鍵管理方法であって、前記クライアントは、該クライアントで作成した前記アプリケーションサーバごとの取引用公開鍵ペアを暗号化するための管理用の暗号鍵を保持し、前記ネットワークには、前記管理用の暗号鍵により暗号化された前記クライアントの取引用公開鍵ペアを格納するための鍵管理サーバを設置することを特徴とする。

## 【0011】

また本発明は、クライアントからネットワーク経由でアプリケーションサーバに接続し各種の取引を行う際に使用する前記クライアントの公開鍵を管理する公開鍵管理方法であって、前記クライアントで、前記アプリケーションサーバごとの取引用公開鍵ペアを暗号化するための管理用の暗号鍵を作成し、保持するステップと、前記クライアントで、前記アプリケーションサーバごとに取引用公開鍵ペアを生成するステップと、前記クライアントで、前記生成した取引用公開鍵ペアを前記管理用暗号鍵で暗号化するステップと、前記暗号化された取引用公開鍵ペアを、前記ネットワークに接続された鍵管理サーバに送信するステップと、前記鍵管理サーバで受信した前記暗号化された取引用公開鍵ペアを所定の記憶手段に格納するステップと、前記クライアントから前記アプリケーションサーバに接続して取引するため、前記鍵管理サーバから前記暗号化された取引用公開鍵ペアを取得するステップと、取得した取引用公開鍵ペアを、前記保持してある管理用暗号鍵で復号するステップと、復号した取引用公開鍵ペアを用いて前記アプリケーションサーバとの取引を実行するステップとを備えたことを特徴とする。

## 【0012】

また本発明は、上述の公開鍵管理方法において、前記鍵管理サーバで、前記取引用公開鍵ペアの有効期限を管理し、該有効期限が満了したとき、または、該有効期限満了前の所定期間に至ったときに、前記クライアントに対して取引用公開鍵ペアの更新を行うべきことを通知するステップを、さらに備えたことを特徴とする。

## 【0013】

また本発明は、上述の公開鍵管理方法において、前記鍵管理サーバで、前記取引用公開鍵ペアの使用回数、最終使用の日時、または使用履歴を管理し、これらの情報に基づいて不正な使用を検出するステップを、さらに備えたことを特徴とする。

## 【0014】

また本発明は、上述の公開鍵管理方法において、不正な使用を検出したとき、前記取引用公開鍵ペアの使用を制限または禁止するステップを、さらに備えたこ



とを特徴とする。

【0015】

また本発明は、上述の公開鍵管理方法において、前記鍵管理サーバに格納する前記取引用公開鍵ペアのうち、公開鍵は平文で格納することを特徴とする。

【0016】

さらに本発明は、上述の公開鍵管理方法において、前記鍵管理サーバに前記クライアントの鍵管理用公開鍵をさらに保管し、前記取引用公開鍵ペアの使用時に、前記鍵管理用公開鍵を用いて個人認証を実施することを特徴とする。

【0017】

上記構成により、各クライアントはサービスを利用するアプリケーションサーバ毎に取引用公開鍵ペアを生成するが、生成した取引用公開鍵ペアは各クライアントが保持・管理するのでなく、鍵管理サーバに登録することにより、各クライアントでの鍵管理が不要となる。また、登録する各クライアントの公開鍵ペアは、個人の管理用暗号鍵（共通鍵または公開鍵ペア）により暗号化して登録することにより、他者に個人の取引用公開鍵ペアを知られることを防ぐことができる。また、鍵管理サーバに登録する際に、各クライアント対応のインデクス及びアプリケーションサーバ対応のインデクスで管理することで、個人が取引時に、取引用公開鍵ペアを鍵管理サーバから取得する際に必要な鍵を特定する。さらに、鍵情報には有効期限、使用回数限度、使用回数、及び最終使用日時を同時に記録しておき、使用条件の検証を行うことにより、不正な使用を検出することができる。

【0018】

【発明の実施の形態】

以下、本発明の実施の形態を図面により詳細に説明する。

【0019】

図1は、本発明の第1の実施形態に係るシステムの構成図で、取引先インデクスを個人クライアントの中に持つ場合の構成である。個人クライアント102、鍵管理サーバ103、アプリケーションサーバ1（120）、及びアプリケーションサーバ2（121）が、ネットワーク111で接続されている。

## 【0020】

個人クライアント102は、個人101が使用するもので、鍵生成部112、暗号処理部113、鍵登録部114、取引判定部115、取引実行部116、及び格納媒体117を備えている。鍵生成部112は、個人の鍵管理用鍵118や取引用公開鍵ペア105、106を生成する。暗号処理部113は、鍵生成部112で生成した取引用公開鍵ペア105、106を鍵管理用鍵118で暗号化したり、鍵管理サーバ103から取得した暗号化された取引用公開鍵ペア105、106を復号する。鍵登録部114は、暗号化された取引用公開鍵ペア105、106を鍵管理サーバ103に登録する。

## 【0021】

取引判定部115は、取引用公開鍵ペア105、106の有効期限や使用回数等の使用条件の報告を鍵管理サーバ103から受け、取引を実施するか判定する。取引実行部116は、取引判定部115の判定で取引を行う場合、鍵管理サーバ103から取得し暗号処理部113で復号化された取引用公開鍵ペア105、106を使用して、アプリケーションサーバ1(120)やアプリケーションサーバ2(121)と取引を実施する。格納媒体117には、鍵管理用鍵118、及び取引用公開鍵ペアがどのアプリケーションサーバと対応したものを示す取引先インデクス119が、格納される。

## 【0022】

鍵管理サーバ103は、鍵格納部104、鍵インデクス部107、鍵登録部108、条件検証部109、及び鍵提供部110を備える。鍵格納部104は、個人クライアント102から登録依頼をうけた取引用公開鍵ペア105、106(個人の鍵管理用鍵118で暗号化されている)を格納する部位である。また鍵使用の履歴122も格納している。鍵インデクス部107は、登録した鍵、個人、及び取引先の関連付けを示すインデクスで、図15(後述)にその内容を示している。鍵登録部108は、個人クライアント102から依頼された取引用公開鍵を鍵格納部104に登録し、鍵インデクス部107を更新する。条件検証部109は、取引用公開鍵105、106の有効期限や使用回数限度などを検証し、期限や限度等が超過していれば、個人クライアント102に連絡する。鍵提供部1

10は、個人クライアント102からの要求により鍵格納部104に登録されている取引用公開鍵ペアを個人クライアント102に送信する。

【0023】

なお、図1の鍵管理用鍵118は、秘密鍵と公開鍵のペアからなるように図示しているが、これに限らず、単一の共通鍵を用いてもよい。後述する図2及び図3のシステムの鍵管理用鍵218、318も同様である。

【0024】

図2は、本発明の第2の実施形態に係るシステムの構成図で、取引先インデックスを鍵管理サーバの中に持つ場合の構成である。図1では個人クライアント102の格納媒体117にあった取引先インデックス部119が、図2では鍵管理サーバ203の中に設けてある。取引先インデックス219は、図1では個人毎にばらばらに存在し、取引先IDもばらばらだった取引先インデックスが、鍵管理サーバ203で1個に統一され、同じアプリケーションサーバであれば、同じ取引先IDを持つことになり、管理し易くなる。なお、図2の200番台の構成要素と図1の100番台の構成要素とは、下2桁が同じ番号の構成要素同士が対応しているものとする。

【0025】

図3は、本発明の第3の実施形態に係るシステムの構成図で、鍵管理サーバに登録した取引用公開鍵ペアのうち公開鍵は暗号化せずに登録する場合の構成である。図2と比べて、鍵管理サーバ303に公開鍵認証部322が追加される。取引用公開鍵ペアのうち公開鍵は暗号化していないので、個人301またはアプリケーションサーバ320、321から個人301の取引用公開鍵について検証依頼があった場合、個人301に問い合わせず、鍵管理サーバ303で認証が可能となる。なお、図3の300番台の構成要素と図2の200番台の構成要素とは、下2桁が同じ番号の構成要素同士が対応しているものとする。

【0026】

図4は、本発明の第4の実施形態に係るシステムの構成図で、個人の鍵管理用公開鍵ペアの公開鍵を暗号化せず鍵管理サーバに登録する場合の構成である。図1～3のシステムでは鍵管理用鍵118、218、318は公開鍵ペアでも共通

鍵でもよかったが、図4では、個人クライアント402の格納媒体417に格納されている鍵管理用鍵418は公開鍵ペアである。また鍵管理サーバ403には個人認証部426が追加され、鍵格納部404には鍵管理用鍵418の公開鍵である鍵管理用公開鍵423が登録されている。個人認証部426は、個人クライアント402からの鍵管理用鍵418の秘密鍵で署名された個人証明書を受け取り、鍵管理用公開鍵423で検証する。

## 【0027】

以下、フローチャートを用いて、上述の実施形態のシステムの動作を説明する。

## 【0028】

図5は、図1のシステムにおける個人の管理用鍵118の生成のフローチャートを示したものである。個人クライアント102において個人の管理用鍵118の生成の開始が指示されると（ステップ501）、図1の個人クライアント102の鍵生成部112において、暗号鍵を生成する（ステップ502）。暗号技術としては、公開鍵暗号技術として既に公知となっているRSA暗号や楕円曲線暗号技術などを利用することができる。また共通鍵暗号の技術も適用可能である。生成した暗号鍵118は格納媒体117に格納する（ステップ503）。ここでは図1のシステムにおける管理用鍵生成の流れを説明したが、図2、及び図3のシステムでも同じである。図4のシステムにおける個人の管理用鍵の生成と登録の流れは、図12で後述する。

## 【0029】

図6は、図1のシステムにおける取引用鍵105、106の生成と登録のフローチャートを示したものである。個人クライアント102において取引用鍵の生成と登録の開始が指示されると（ステップ601）、図1の個人クライアント102の鍵生成部112で取引用の公開鍵ペアを生成する（ステップ602）。次に、この公開鍵ペアを使用するアプリケーションサーバが格納媒体117に格納されている取引先インデクス部119に登録されているか否か検索し（ステップ603）、登録されていなければ新規取引先として取引先インデクス部119に追加する（ステップ604）。

## 【0030】

次に、取引先インデクス番号（取引先ID）を取得する（ステップ605）。ステップ602で生成した取引用公開鍵ペアを、格納媒体117に格納されている管理用鍵118で、暗号化する（ステップ606）。この暗号化した取引用公開鍵ペアと個人ID、取引先ID、及び鍵の有効期限や使用回数限度などの使用条件を管理サーバ103に送信し鍵格納部104に登録する（ステップ607）。なお、図2～図4のシステムにおける取引用鍵の生成と登録の流れは、図10を参照して後述する。

## 【0031】

図7は、図1のシステムにおける取引の実行のフローチャートを示したものである。個人クライアント102において取引の実行の開始が指示されると（ステップ701）、まず個人クライアント102の格納媒体117に格納されている取引先インデクス部119を検索して使用するアプリケーションサーバの取引先インデクス番号（取引先ID）を取得する（ステップ702）。例えば図16の取引先インデクスでは、「A銀行との取引であれば、取引先IDは001」というように個人101が取引毎に特定することができる。次に鍵管理サーバ103に個人IDと取引先IDを送信して取引用公開鍵ペアの取得を要求する（ステップ703）。取得した取引用公開鍵ペアは暗号化されているため、個人管理用鍵118を使用して復号化する（ステップ704）。復号化された取引用公開鍵を使用して、アプリケーションサーバと取引を実行する（ステップ706）。

## 【0032】

ここでの取引の実行は公知の公開鍵暗号技術を使用した取引で、例えばVisa InternationalとMasterCard Internationalの策定したSET (Secure Transaction Protocol)のような取引方式が利用できる。

## 【0033】

なお、ここでは図1のシステムにおける取引実行の流れを説明したが、図2及び図3のシステムでも同様である。ただし、図2及び図3のシステムでは取引先インデクス部が鍵管理サーバ内に設けられているので、ステップ702の処理では鍵管理サーバの取引先インデクスを検索することになる。あるいは、鍵管理サ

ーバに取引先名称などの取引先インデックスを検索するキーとなる情報を渡し、鍵管理サーバ側で取引先IDを求めて取引用公開鍵ペアの検索に利用してもよい。

図4のシステムにおける取引実行の流れは、図13で後述する。

#### 【0034】

図8は、図1のシステムにおける鍵管理サーバ103の条件検証部109で、有効期限のチェックと満了の通知をする場合のフローチャートを示したものである。鍵管理サーバ103における条件検証（有効期限の通知）の処理（ステップ801）では、個人クライアント102からの取引用公開鍵ペア登録依頼の際、同時に送信される鍵の有効期限を図15に示す鍵インデックス107に登録する（ステップ802）。

#### 【0035】

その後、所定時間間隔でタイマー通知のプロセス（ステップ804）を繰り返し実行する。このタイマー通知では、鍵インデックス部107に登録されているすべての取引用公開鍵ペアの有効期限をチェックし（ステップ805）、有効期限を超過している取引用公開鍵ペアがあれば、その所有者である個人クライアントに有効期限満了を通知する（ステップ806）。これにより、個人101は個人取引用鍵の有効期限満了を随時意識する必要が無く、通知を受けた時点で取引用公開鍵の生成(更新)を実行することで継続して有効な公開鍵を維持することができる。

#### 【0036】

ここでは図1のシステムにおける条件検証処理の流れを説明したが、図2～図4のシステムでも同様である。また、ここでは有効期限が満了したときに通知しているが、有効期限の満了前の所定期間に至ったときに通知するようにしてもよい。

#### 【0037】

図9は、図1のシステムにおける鍵管理サーバ103の条件検証部109で、使用回数のチェックとその限度超過の通知をする場合のフローチャートを示したものである。予め、個人クライアント102からの取引用公開鍵ペア登録依頼の際、同時に送信される鍵の使用回数限度を図15に示す鍵インデックス107に登

録しておく。図15のように、累積使用回数限度1510、1日使用回数限度1511、1週間使用回数限度1512、及び1月使用回数限度1513を登録すれば、時間単位の管理が可能である。状況により別の時間単位にすることも可能である。

#### 【0038】

図9の鍵管理サーバ103での条件検証（使用回数限度の通知）処理は、個人クライアントから取引用公開鍵ペアの送付要求が来た場合に起動する。本処理が開始すると（ステップ901）、取引用公開鍵ペアの使用、すなわち取引用公開鍵ペアを個人クライアントに送付し（ステップ902）、その鍵の使用回数1505～1507を+1更新（カウントアップ）する（ステップ903）。このとき、現在時点が、1日、1週間、あるいは1月の使用回数をカウントする時間区間の区切りに至っていたときは、その使用回数のカウンタ1505～1507をゼロクリアした後、カウントアップするものとする。次に、それぞれの時間単位（1日、1週間、1月）の使用回数限度をチェックし（ステップ904）、超過していれば当該取引用公開鍵ペアの所有者の個人クライアントに使用回数限度超過を連絡する（ステップ905）。この際、使用回数、最終使用時刻、及び使用履歴も要求により送付する。

#### 【0039】

個人101は、この使用回数限度超過の通知を受信すると、自分自身で記録している使用回数、最終使用時刻、及び使用履歴と比較し、不正使用の有無を判定する。不正使用と判定した場合は、鍵管理サーバ103に登録してある取引用鍵の変更、鍵管理サーバ103のパスワード等の認証情報の変更が必要である。また使用回数限度超過報告（ステップ905）が送信される場合だけでなく、必要な場合に鍵管理サーバ103に問い合わせし、使用回数、最終使用時刻、及び使用履歴等の使用状況情報を取得して、個人101がその都度不正使用を判定することも可能である。

#### 【0040】

ここでは図1のシステムにおける条件検証処理の流れを説明したが、図2～図4のシステムでも同様である。

## 【 0 0 4 1 】

図 1 0 は、図 3 のシステムにおける取引用鍵 3 0 5, 3 0 6 の生成と登録の流れ、すなわち取引先インデクス部 3 1 9 を鍵管理サーバ 3 0 3 に持ち取引用鍵のうち秘密鍵のみ暗号化する場合のフローチャートを示したものである。ステップ 1 0 0 2, 1 0 0 3 は図 6 のステップ 6 0 2, 6 0 3 と、ステップ 1 0 0 4 ~ 1 0 0 8 は図 6 のステップ 6 0 3 ~ 6 0 7 と、同様の処理である。図 6 との相違は、取引先インデクスを検索する場合、個人クライアントの取引先インデクスでなく、鍵管理サーバ 3 0 3 の取引先インデクス 3 1 9 を検索し（ステップ 1 0 0 3）、取引用公開鍵ペア 3 0 5, 3 0 6 の暗号化は秘密鍵のみを個人管理用鍵 3 1 8 で暗号化することである（ステップ 1 0 0 7）。

## 【 0 0 4 2 】

取引先インデクス部 3 1 9 が鍵管理サーバ 3 0 3 にあることにより、サーバ側で取引先毎の管理が容易になる。なお、ここでは図 3 のシステムにおける取引用鍵の生成と登録の流れを説明したが、図 2 及び図 4 のシステムでも同様である。ただし、図 2 のシステムでは取引用公開鍵ペア 2 0 5, 2 0 6 は秘密鍵と公開鍵の両方を個人管理用鍵 2 1 8 で暗号化するためステップ 1 0 0 7 では秘密鍵だけでなく公開鍵も暗号化する。

## 【 0 0 4 3 】

図 1 1 は、図 3 のシステムにおいて図 1 0 で暗号化せずに登録した取引用公開鍵ペア 3 0 5, 3 0 6 の公開鍵の認証を鍵管理サーバ 3 0 3 で行う場合のフローチャートを示したものである。ここではアプリケーションサーバ 1 ( 3 2 0 ) から個人 3 0 1 の取引用公開鍵の検証を依頼された場合について説明する。取引用公開鍵の認証が開始されると（ステップ 1 1 0 1）、検証を依頼されたアプリケーションサーバ 1 ( 3 2 0 ) から取引用公開鍵の検証依頼を受け付け（ステップ 1 1 0 2）、取引先インデクス 3 1 9 からアプリケーションサーバ 1 ( 3 2 0 ) と個人 ID の該当する取引用公開鍵ペアを検索し、その公開鍵を見つけ出す（ステップ 1 1 0 3）、この公開鍵とアプリケーションサーバ 1 ( 3 2 0 ) から送付された公開鍵とを比較し（ステップ 1 1 0 4）、一致すれば認証したことをアプリケーションサーバ 1 ( 3 2 0 ) に連絡する（ステップ 1 1 0 6）。不一致であ



れば否認を連絡する（ステップ1107）。なお、図4のシステムも同様の処理である。

#### 【0044】

図12は、図4のシステムにおける個人の管理用鍵418の生成と登録の流れ、すなわち公開鍵ペア418の公開鍵を鍵管理サーバ403に鍵423として登録する場合のフローチャートを示したものである。ステップ1202、1203は図5のステップ502、503と同様の処理である。図5との相違は、個人管理用鍵の生成が必ず公開鍵ペア（公開鍵と秘密鍵）であること（ステップ1202）、及び個人管理用公開鍵ペア418のうち公開鍵を鍵管理サーバに鍵423として登録する（ステップ1204）ことである。

#### 【0045】

図13は、図4のシステムの個人クライアント402における取引の実行のフローチャートを示したものである。ステップ1304～1306は図7のステップ703～705と同様の処理である。図7との相違は、取引を開始する前に個人管理用公開鍵ペア418の秘密鍵で個人証明書に署名し、鍵管理サーバ403に送付することである（ステップ1302）。鍵管理サーバから個人認証OKで返ってくれば（ステップ1303）、以降は図7と同様である。個人認証NGであれば、取引処理はできない。

#### 【0046】

図14は、図4のシステムの鍵管理サーバ403での個人認証のフローチャートを示したものである。鍵管理サーバ403の個人認証処理が開始されると（ステップ1401）、個人クライアント402から図13で示したように個人証明書を受け付け（ステップ1402）、鍵管理サーバ403に登録されている鍵管理用公開鍵423を使用して、送付された個人証明書の署名を検証する（ステップ1403）。検証OKであれば、個人認証OKを個人クライアント402に返信し（ステップ1405）、当該個人IDからの取引用公開鍵取得要求を許可状態にする（ステップ1406）。検証NGであれば、個人認証の否認を個人クライアント402に返信し（ステップ1407）、当該個人IDからの取引用公開鍵取得要求を不許可状態にする（ステップ1408）。図15は、鍵インデック

スに許可、不許可状態を示すフラグ 1 5 0 8 を持つ場合の例である。

【 0 0 4 7 】

図 1 5 は、鍵管理サーバに持つ鍵インデクスの例である。この鍵インデクスは、取引用公開鍵ペアを識別する鍵 ID 1 5 0 1、所有者を識別する個人 ID 1 5 0 2、取引先のアプリケーションサーバを識別する取引先 ID 1 5 0 3、鍵の累積の使用回数を示すカウンタ 1 5 0 4、1 日の使用回数を示すカウンタ 1 5 0 5、1 週間の使用回数を示すカウンタ 1 5 0 6、1 ヶ月の使用回数を示すカウンタ 1 5 0 7、この鍵の使用が許可されているか否かの状態を示す状態フラグ 1 5 0 8、最後に使用した日時を示す領域 1 5 0 9、鍵の有効期限を示す設定領域 1 5 1 0、累積の使用回数限度を示す設定領域 1 5 1 1、1 日の使用回数限度を示す設定領域 1 5 1 2、1 週間の使用回数限度を示す設定領域 1 5 1 3、及び 1 ヶ月の使用回数限度を示す設定領域 1 5 1 4 などからなる。

【 0 0 4 8 】

図 1 6 は、取引先インデクスの例である。取引先インデクスは、取引先のアプリケーションサーバを識別するための取引先 ID 1 6 0 1、取引先の名称 1 6 0 2、アプリケーションサーバの名称 1 6 0 3、及び業務内容 1 6 0 4 などからなる。図 1 の例では取引先インデクスを個人クライアントに持つため、同一のアプリケーションサーバであっても取引先 ID は個人毎にばらばらである。図 2、図 3、図 4 では鍵管理サーバで管理するため、同一のアプリケーションサーバの取引先 ID は同一である。

【 0 0 4 9 】

図 1 7 は、鍵管理サーバで持つ管理用の鍵インデクスの例である。管理用の鍵インデクスは、管理用鍵の識別をするための個人管理用鍵 ID 1 7 0 1、所有者を識別するための個人 ID 1 7 0 2、及び暗号種別などの管理用鍵の付加情報を示す管理用鍵情報 1 7 0 3 からなる。

【 0 0 5 0 】

なお、上記実施形態ではネットワーク経由の安全な取引を行う場合を想定しており、基礎技術として公開鍵暗号技術を想定している。公開鍵暗号は秘密鍵と公開鍵の 2 つの鍵をペアで使用する暗号技術であり、秘密鍵を他者に知られること

なく管理することで安全が維持されている。公開鍵暗号技術に関連して公開鍵と秘密鍵を保持している者を認証するために認証局を使用する方式も普及している。この場合、公開鍵に対応して電子認証書を認証局が発行し、取引時には秘密鍵・公開鍵に加え、電子認証書を使用することでさらに安全が高まる。本発明は、電子認証書も公開鍵と組み合わせて管理することに容易に拡張することができる。

#### 【0051】

##### 【発明の効果】

以上説明したように、本発明によれば、各クライアントは1個の鍵管理用鍵を管理するだけで、セキュリティを確保しながらアプリケーションサーバごとの取引用鍵を扱うことができる。したがって、各クライアントでの鍵管理は容易であり、携帯端末からの取引も容易に行える。また、鍵管理サーバで、鍵使用条件の検証、取引用鍵の検証、及び公開鍵技術を使用した個人の認証も可能である。

##### 【図面の簡単な説明】

##### 【図1】

本発明の第1の実施形態のシステムの構成図である。

##### 【図2】

本発明の第2の実施形態のシステムの構成図である。

##### 【図3】

本発明の第3の実施形態のシステムの構成図である。

##### 【図4】

本発明の第4の実施形態のシステムの構成図である。

##### 【図5】

個人クライアントにおける個人の管理用鍵生成のフローチャート図である。

##### 【図6】

個人クライアントにおける取引用鍵の生成と登録のフローチャート図である。

##### 【図7】

個人クライアントにおける取引の実行のフローチャート図である。

##### 【図8】

鍵管理サーバにおける条件検証（有効期限の通知）のフローチャート図である。

【図 9】

鍵管理サーバにおける条件検証（使用回数限度の通知）のフローチャート図である。

【図 1 0】

個人クライアントにおける取引用鍵の生成と登録のフローチャート図である。

【図 1 1】

鍵管理サーバにおける取引用公開鍵の認証のフローチャート図である。

【図 1 2】

個人クライアントにおける個人の管理用公開鍵の生成と鍵管理サーバへの登録のフローチャート図である。

【図 1 3】

取引用公開鍵ペア取得のための個人認証後、取引の実行を行う場合のフローチャート図である。

【図 1 4】

鍵管理サーバでの個人認証処理のフローチャート図である。

【図 1 5】

取引用鍵インデックスの形式を示す図である。

【図 1 6】

取引先インデックスの形式を示す図である。

【図 1 7】

個人の管理用公開鍵のインデックスの形式を示す図である。

【符号の説明】

1 0 1 …個人

1 0 2 …個人クライアント

1 0 3 …鍵管理サーバ

1 0 4 …鍵管理サーバの鍵格納領域

1 0 5 …個人取引用公開鍵ペア 1（公開鍵と秘密鍵伴に暗号化）

- 106…個人取引用公開鍵ペア2（公開鍵と秘密鍵伴に暗号化）
- 107…取引用鍵インデクス
- 108…鍵管理サーバの鍵登録部（個人取引用公開鍵ペア）
- 109…鍵管理サーバの条件検証部（有効期限、使用回数限度）
- 110…鍵管理サーバの鍵提供部
- 111…ネットワーク
- 112…個人クライアントの鍵生成部
- 113…個人クライアントの暗号処理部
- 114…個人クライアントの鍵登録部
- 115…個人クライアントの取引判定部
- 116…個人クライアントの取引実行部
- 117…格納媒体
- 118…個人クライアントの個人鍵管理用鍵
- 119…個人クライアントの取引先インデクス
- 120…アプリケーションサーバ1
- 121…アプリケーションサーバ2
- 122…鍵使用履歴部
- 201…個人
- 202…個人クライアント
- 203…鍵管理サーバ
- 204…鍵管理サーバの鍵格納領域
- 205…個人取引用公開鍵ペア1（公開鍵と秘密鍵伴に暗号化）
- 206…個人取引用公開鍵ペア2（公開鍵と秘密鍵伴に暗号化）
- 207…取引用鍵インデクス
- 208…鍵管理サーバの鍵登録部（個人取引用公開鍵ペア）
- 209…鍵管理サーバの条件検証部（有効期限、使用回数限度）
- 210…鍵管理サーバの鍵提供部
- 211…ネットワーク
- 212…個人クライアントの鍵生成部

- 2 1 3 …個人クライアントの暗号処理部
- 2 1 4 …個人クライアントの鍵登録部
- 2 1 5 …個人クライアントの取引判定部
- 2 1 6 …個人クライアントの取引実行部
- 2 1 7 …格納媒体
- 2 1 8 …個人クライアントの個人鍵管理用鍵
- 2 1 9 …鍵管理サーバ内の取引先インデクス
- 2 2 0 …アプリケーションサーバ 1
- 2 2 1 …アプリケーションサーバ 2
- 2 2 2 …鍵使用履歴部
- 3 0 1 …個人
- 3 0 2 …個人クライアント
- 3 0 3 …鍵管理サーバ
- 3 0 4 …鍵管理サーバの鍵格納領域
- 3 0 5 …個人取引用公開鍵ペア 1 (秘密鍵のみ暗号化)
- 3 0 6 …個人取引用公開鍵ペア 2 (秘密鍵のみ暗号化)
- 3 0 7 …取引用鍵インデクス
- 3 0 8 …鍵管理サーバの鍵登録部 (個人取引用公開鍵ペア)
- 3 0 9 …鍵管理サーバの条件検証部 (有効期限、使用回数限度)
- 3 1 0 …鍵管理サーバの鍵提供部
- 3 1 1 …ネットワーク
- 3 1 2 …個人クライアントの鍵生成部
- 3 1 3 …個人クライアントの暗号処理部
- 3 1 4 …個人クライアントの鍵登録部
- 3 1 5 …個人クライアントの取引判定部
- 3 1 6 …個人クライアントの取引実行部
- 3 1 7 …格納媒体
- 3 1 8 …個人クライアントの個人鍵管理用鍵
- 3 1 9 …鍵管理サーバ内の取引先インデクス

- 3 2 0 …アプリケーションサーバ 1
- 3 2 1 …アプリケーションサーバ 2
- 3 2 2 …鍵管理サーバの個人公開鍵認証部
- 3 2 3 …鍵使用履歴部
- 4 0 1 …個人
- 4 0 2 …個人クライアント
- 4 0 3 …鍵管理サーバ
- 4 0 4 …鍵管理サーバの鍵格納領域
- 4 0 5 …個人取引用公開鍵ペア 1（秘密鍵のみ暗号化）
- 4 0 6 …個人取引用公開鍵ペア 2（秘密鍵のみ暗号化）
- 4 0 7 …取引用鍵インデクス
- 4 0 8 …鍵管理サーバの鍵登録部（個人取引用公開鍵ペア）
- 4 0 9 …鍵管理サーバの条件検証部（有効期限、使用回数限度）
- 4 1 0 …鍵管理サーバの鍵提供部
- 4 1 1 …ネットワーク
- 4 1 2 …個人クライアントの鍵生成部
- 4 1 3 …個人クライアントの暗号処理部
- 4 1 4 …個人クライアントの鍵登録部
- 4 1 5 …個人クライアントの取引判定部
- 4 1 6 …個人クライアントの取引実行部
- 4 1 7 …格納媒体
- 4 1 8 …個人クライアントの個人鍵管理用公開鍵ペア
- 4 1 9 …鍵管理サーバ内の取引先インデクス
- 4 2 0 …アプリケーションサーバ 1
- 4 2 1 …アプリケーションサーバ 2
- 4 2 2 …鍵管理サーバの個人公開鍵認証部
- 4 2 3 …個人鍵管理用公開鍵ペアの公開鍵
- 4 2 4 …個人鍵管理用公開鍵のインデクス
- 4 2 5 …個人クライアントの署名生成部

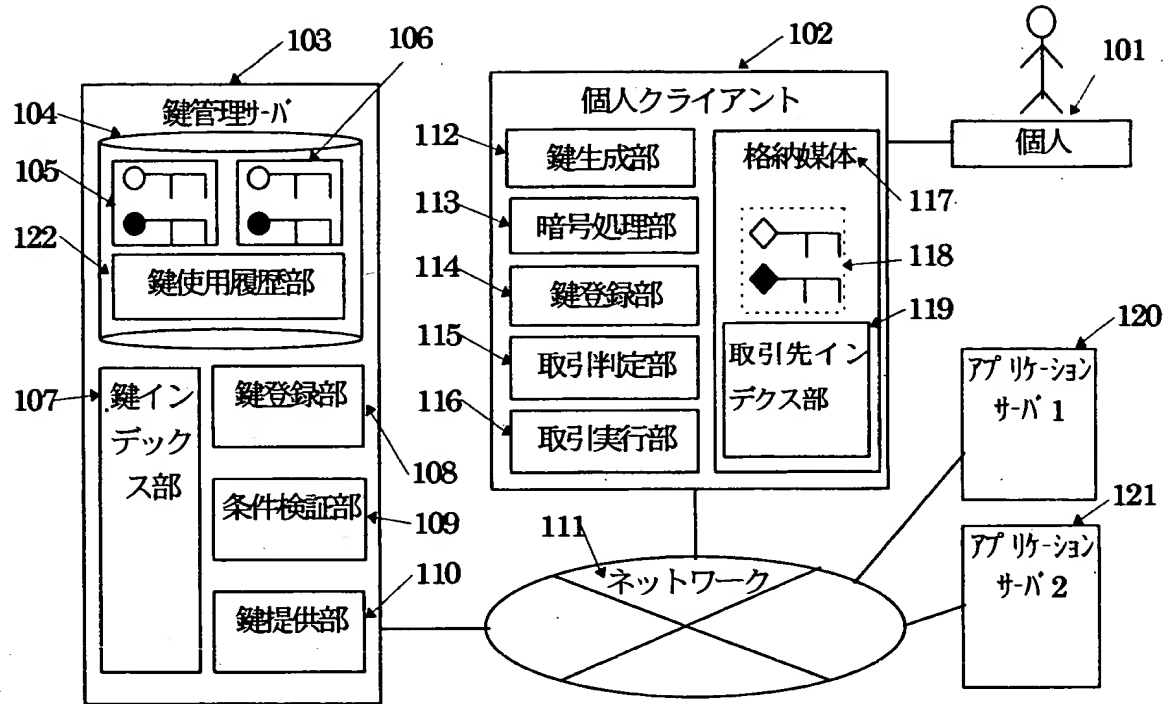
4 2 6 …鍵管理サーバの個人認証部

4 2 7 …鍵使用履歴部

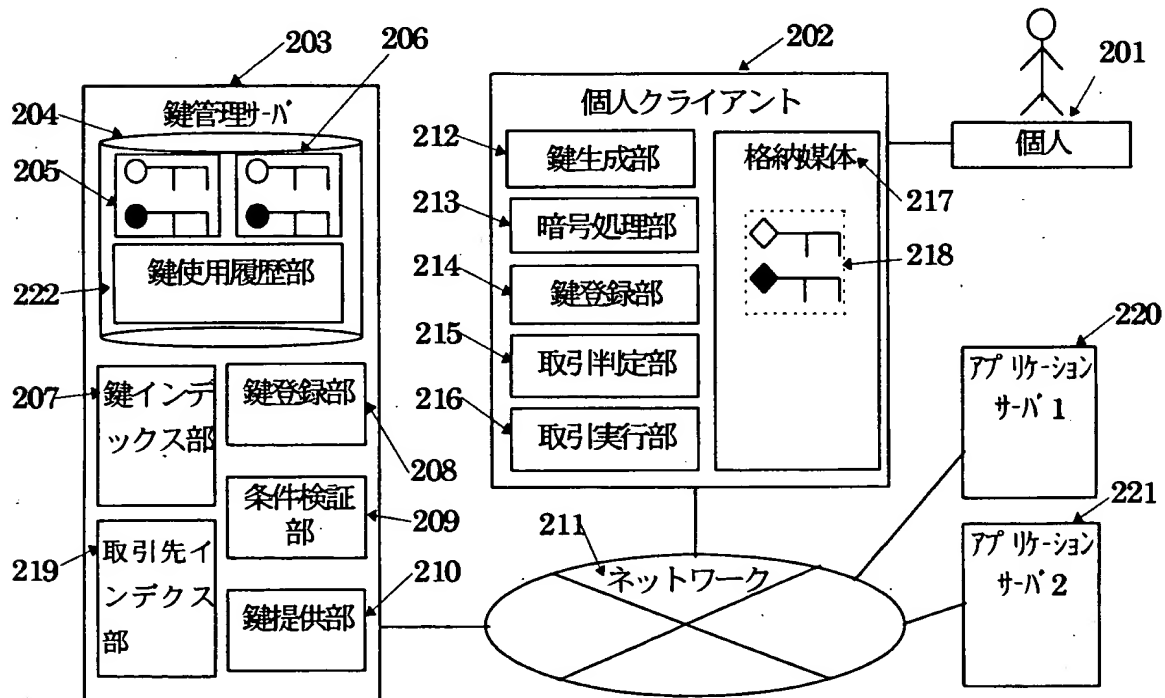


【書類名】 図面

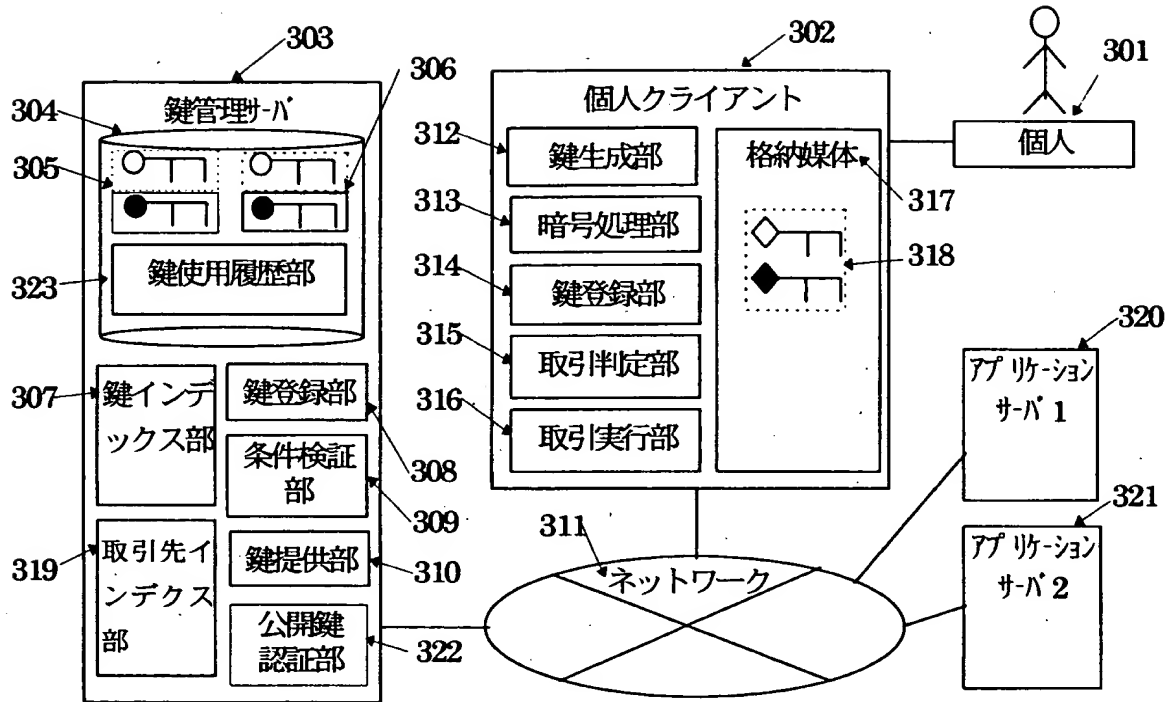
【図 1】



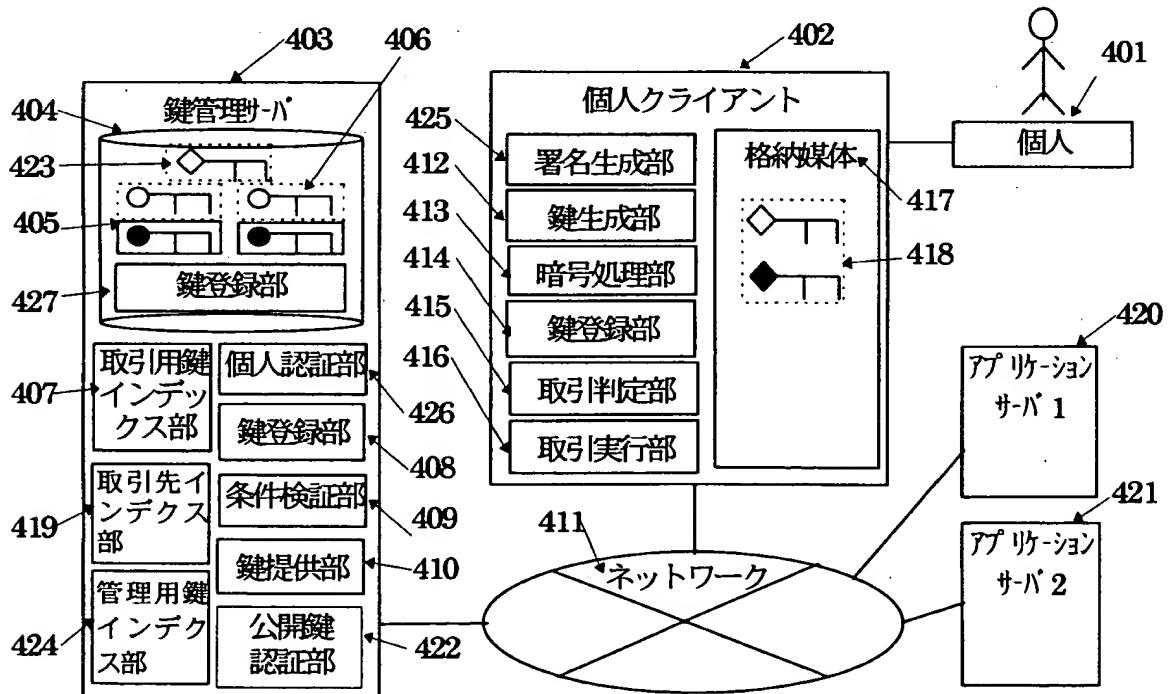
【図 2】



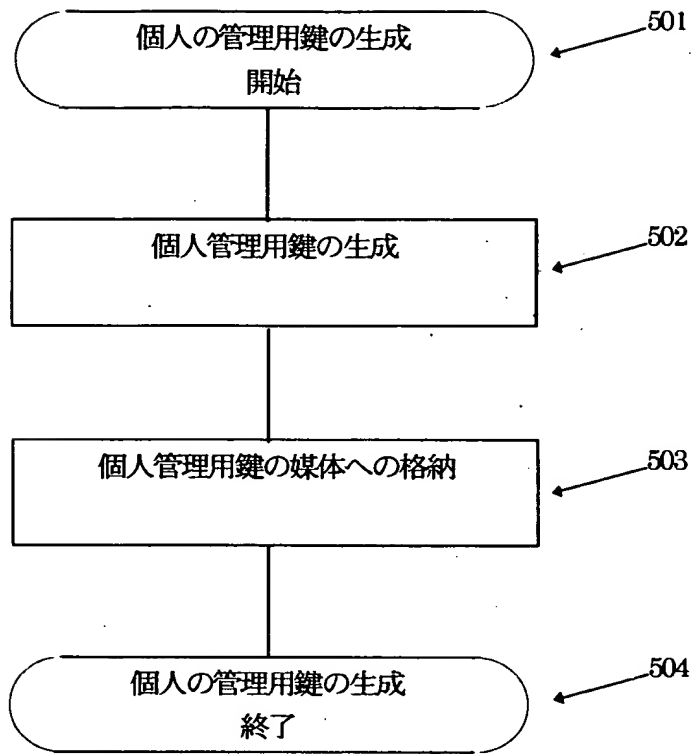
【図 3】



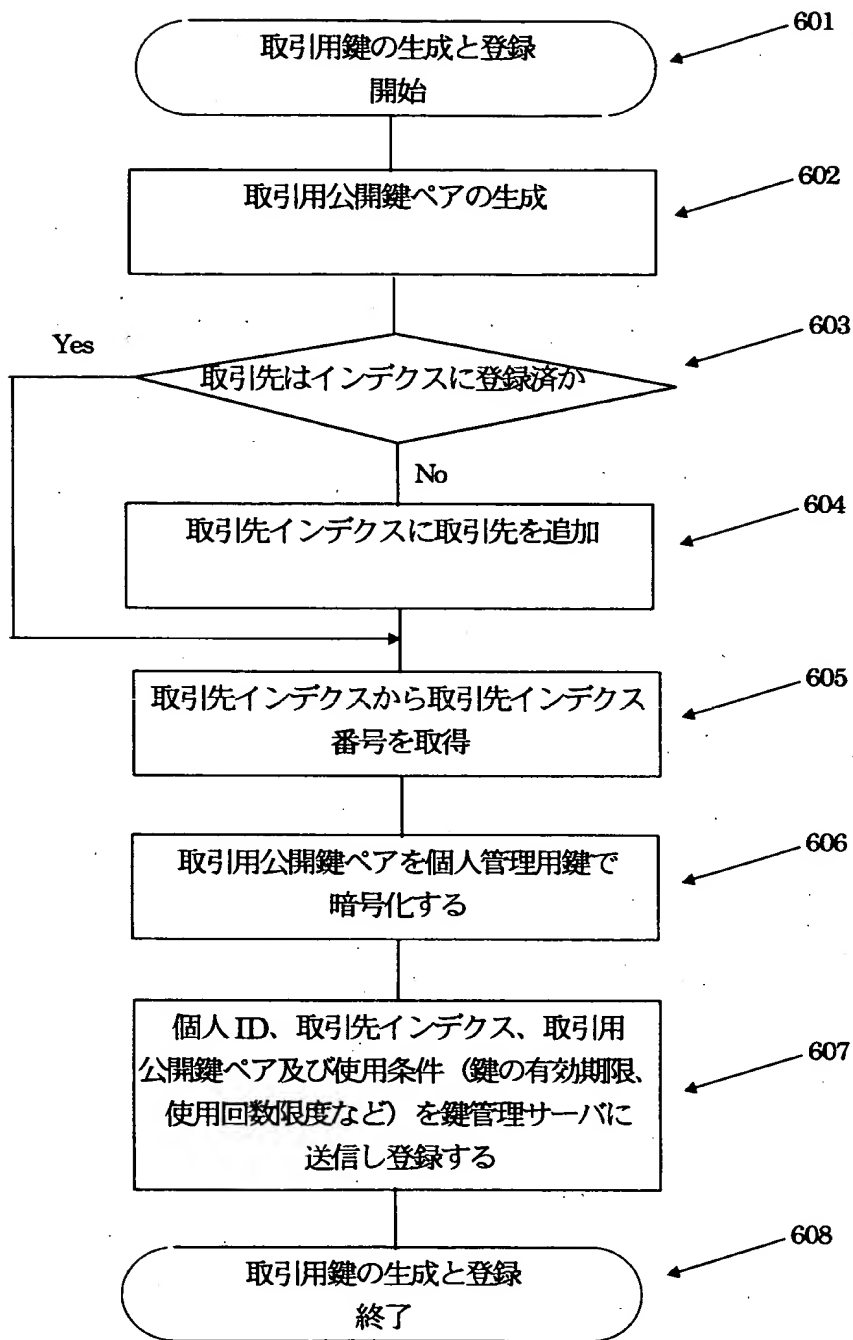
【図 4】



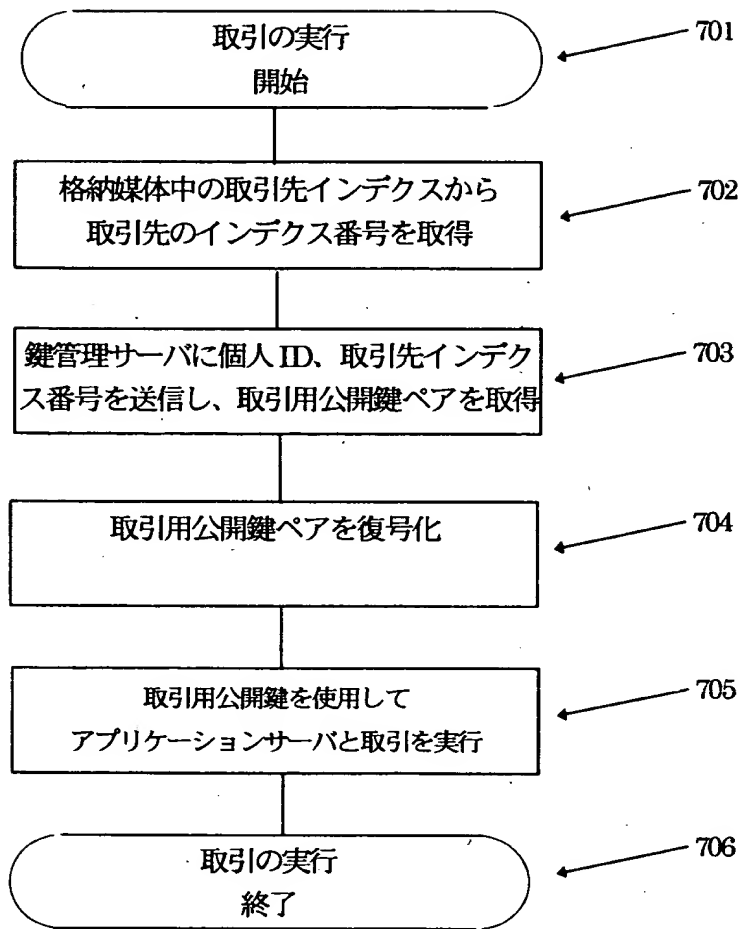
【図 5】



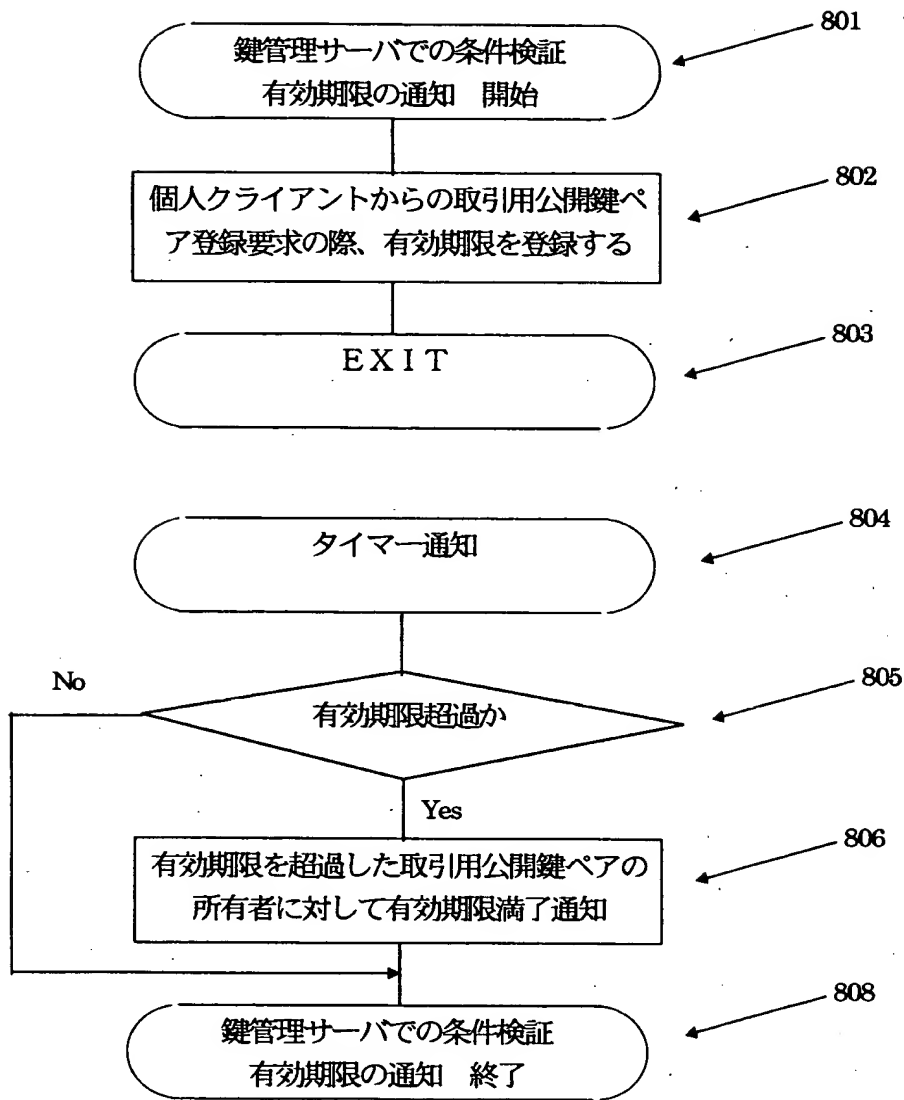
【図 6】



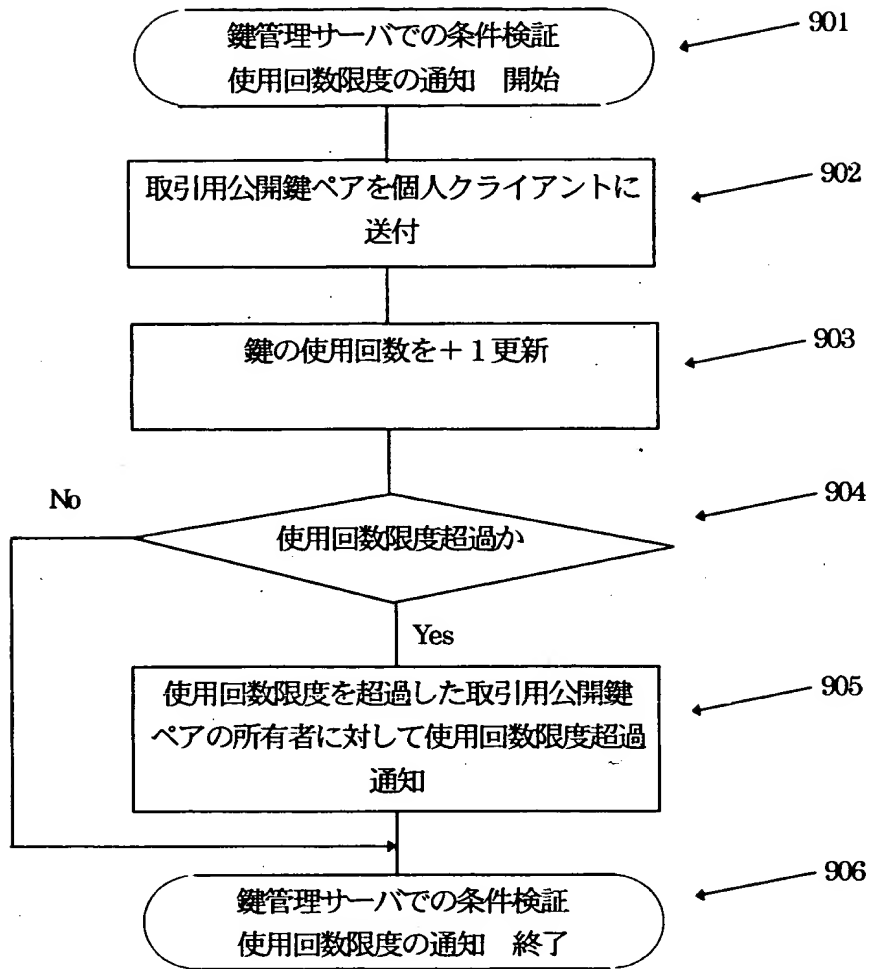
【図 7】



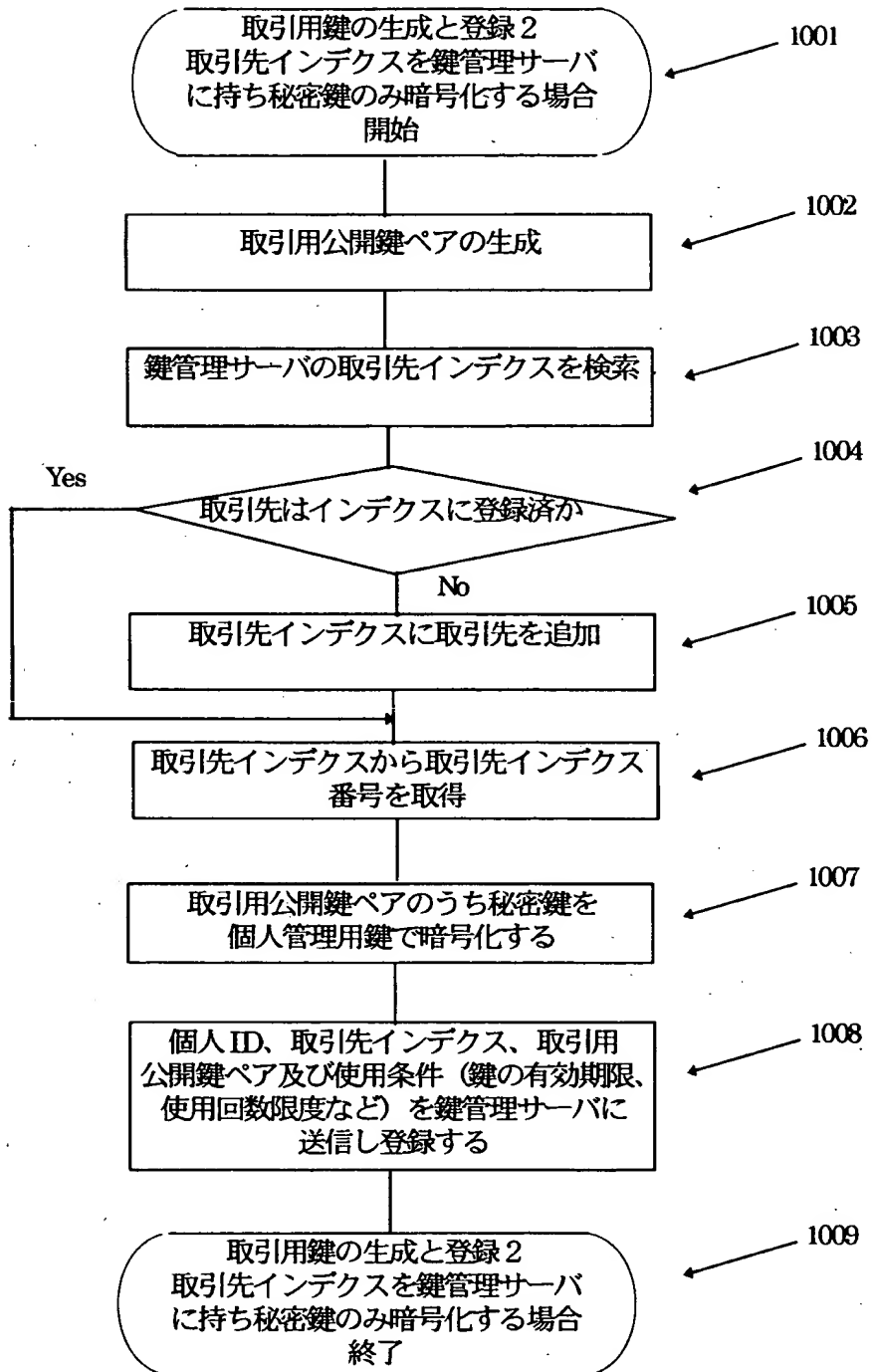
【図 8】



【図 9】

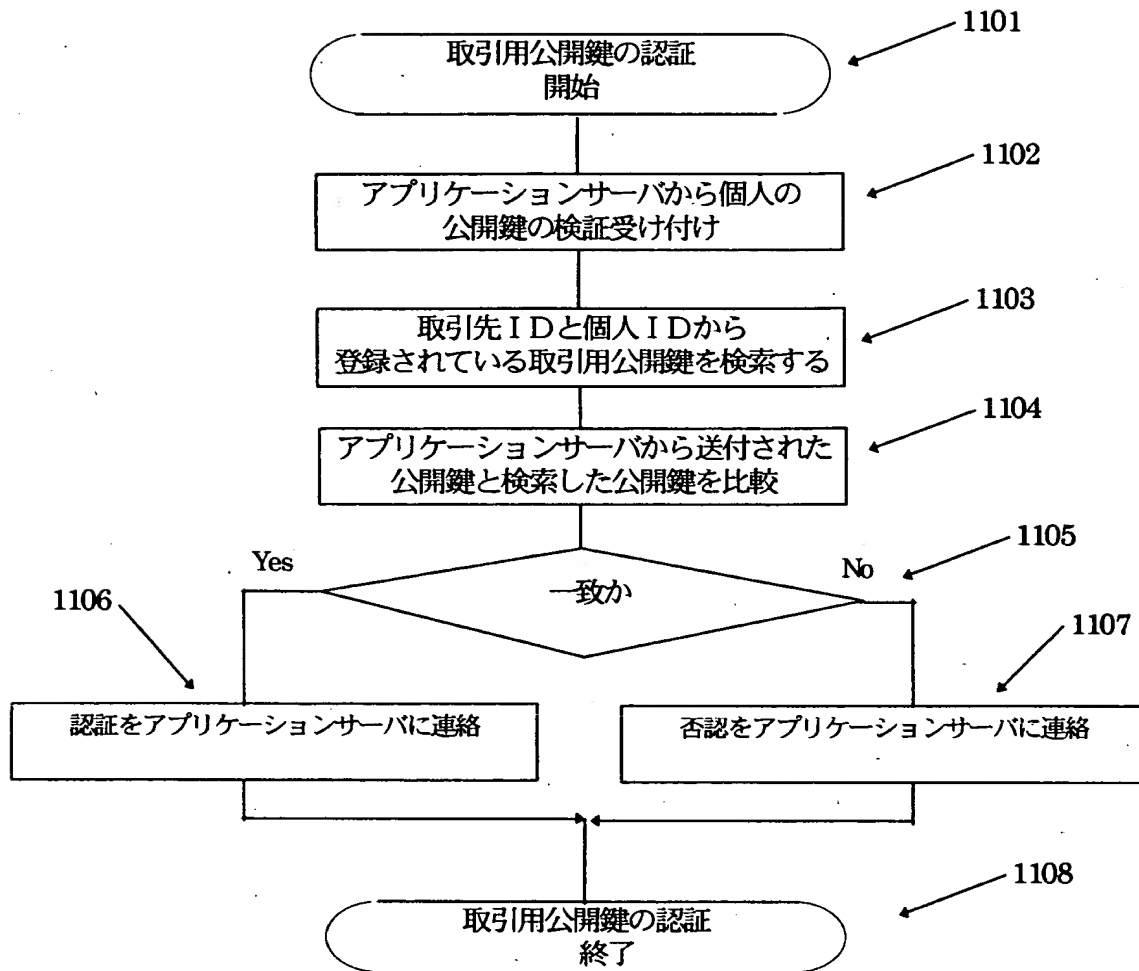


【図 10】

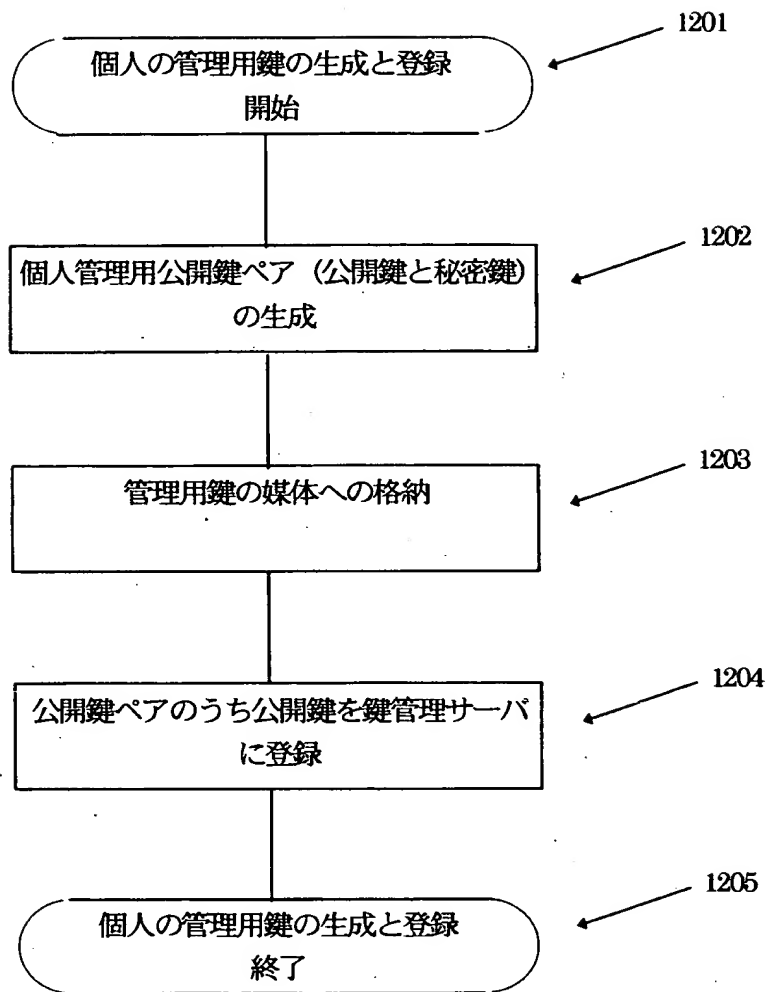




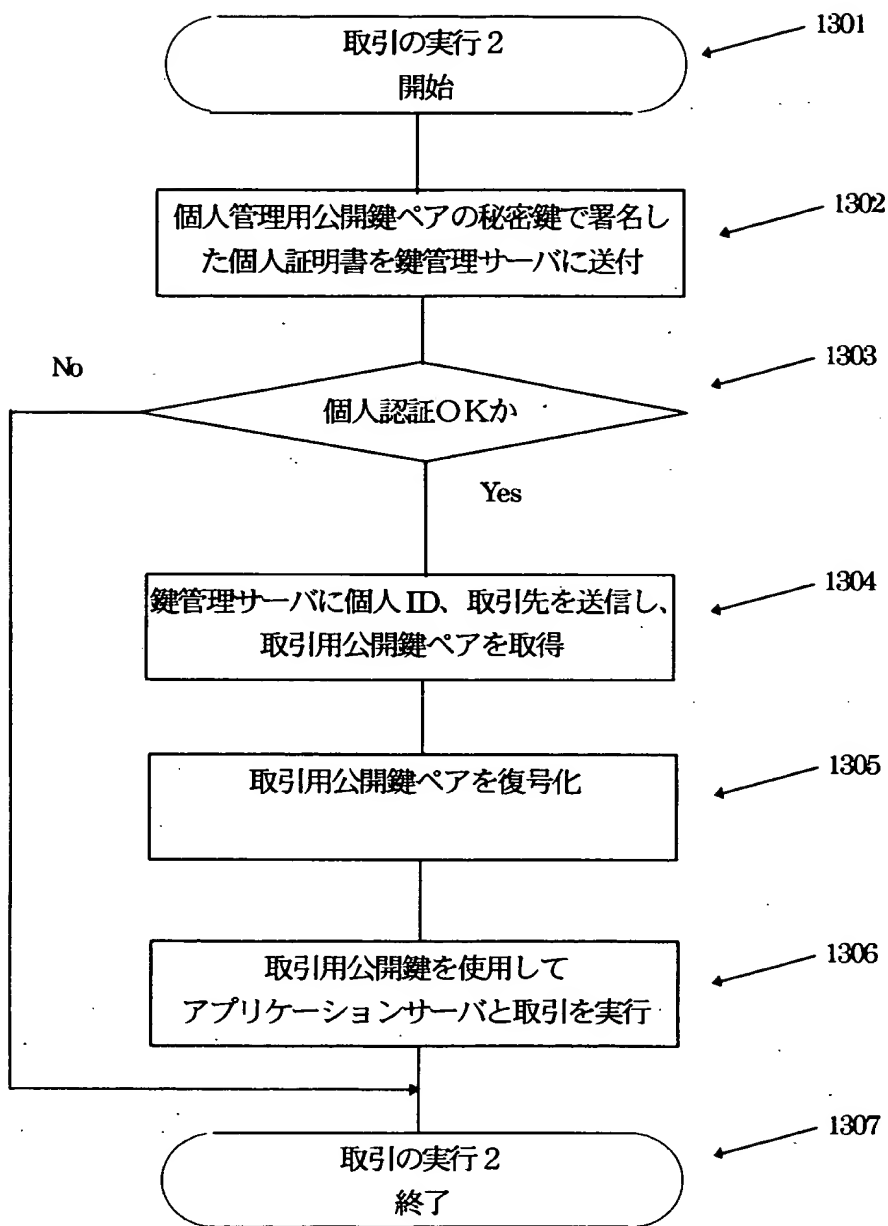
【図 11】



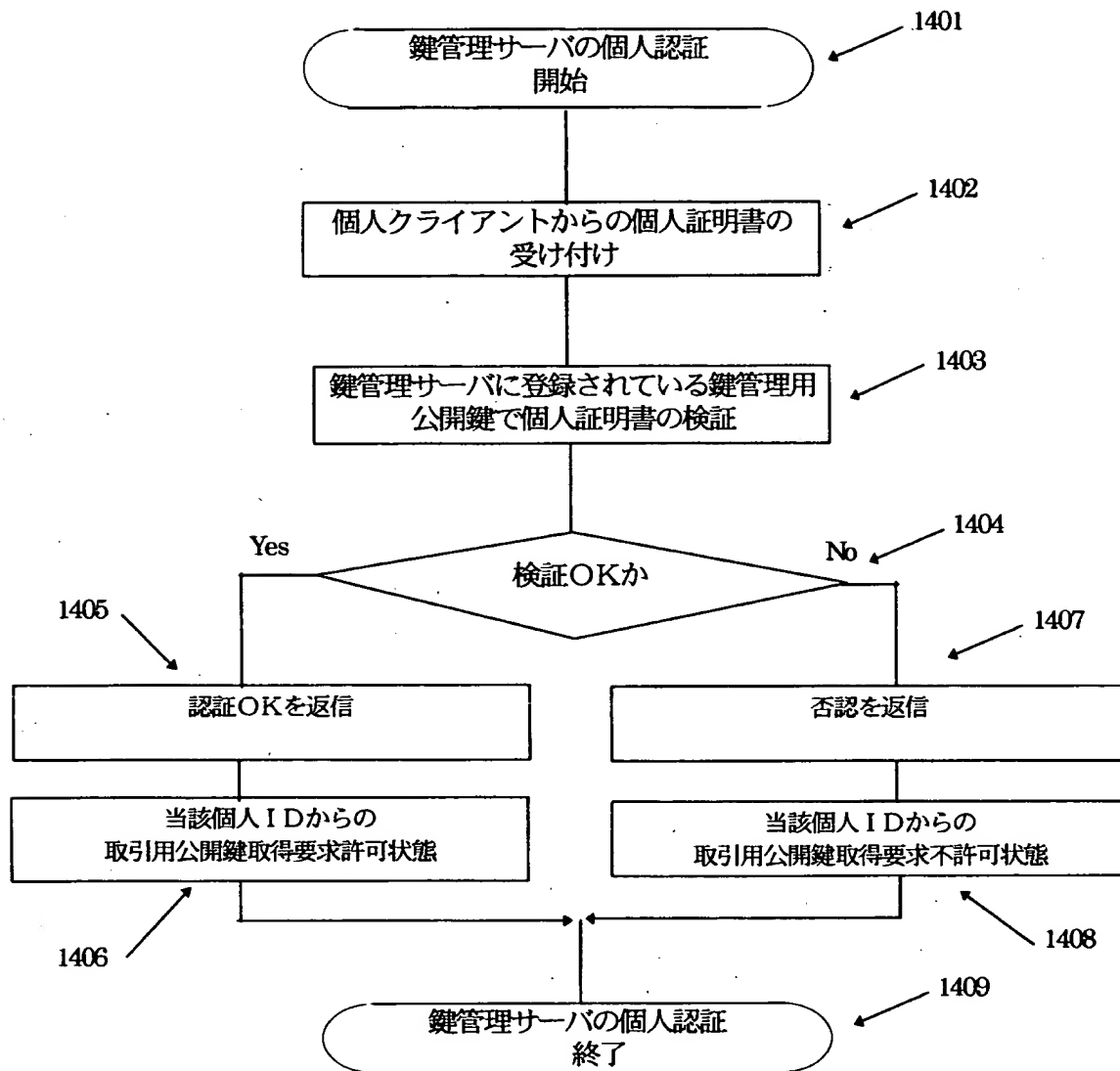
【図 12】



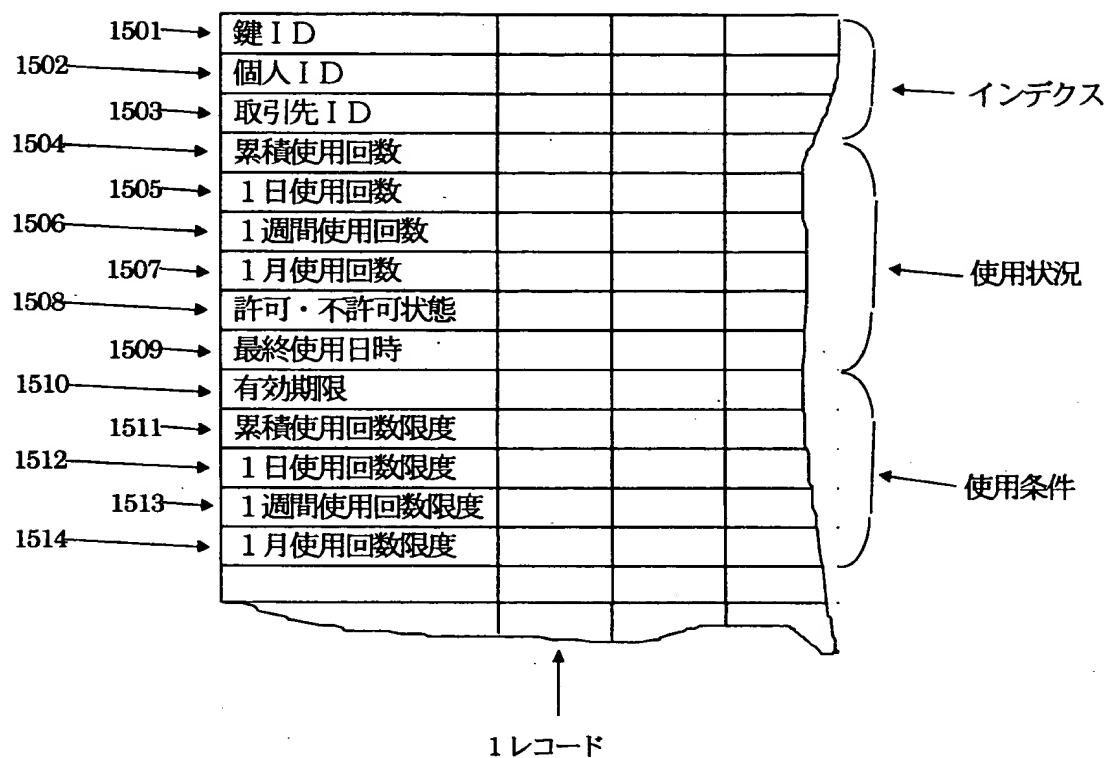
【図 1 3】



【図 1 4】



【図 15】



【図 16】

取引先ID	取引先名称	アプリケーション サーバ名称	業務名称
001	A銀行	APAAA	業務1
002	B信販	APBBB	業務2

【図 17】

個人管理用鍵ID	個人ID	管理用鍵情報	
001			
002			

【書類名】 要約書

【要約】

【課題】

ネットワークを利用して電子商取引等の相手を特定するための認証が必要になるサービスにおいて、サービスを提供するアプリケーションサーバ毎に、個人が取引用公開鍵ペアを管理するような場合の鍵管理の負担を軽減する。この際、セキュリティも確保しておく必要がある。また取引を行うアプリケーションサーバの数が増えても、個人の端末に必要な容量は増せない。

【解決手段】

アプリケーションサーバ毎の取引用公開鍵ペアを個人が保持・管理せずに、鍵管理サーバに登録することにより、個人の鍵管理を不要にする。また登録する取引用公開鍵ペアは、個人の鍵管理用鍵で暗号化することにより、セキュリティを確保する。鍵管理サーバに登録する鍵と共にいろいろな付加情報を登録することにより、多くの付加サービスが可能となる。

【効果】

個人の鍵管理の負荷が軽減する。また取引先のアプリケーションサーバが増えても、個人端末の容量は増えない。このときの取引用鍵のセキュリティも確保できる。また鍵管理に付加するいろいろなサービスがすべての個人に実施できる。

【選択図】 図1

認定・付加情報

特許出願の番号	特願2001-071581
受付番号	50100360167
書類名	特許願
担当官	第七担当上席 0096
作成日	平成13年 3月15日

<認定情報・付加情報>

【提出日】	平成13年 3月14日
-------	-------------



出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地  
氏 名 株式会社日立製作所